ROBERT SHERMAN

CISO
AMERICAN TOWER

HEADQUARTERS: Boston, MA

EMPLOYEES: 6,000+

REVENUE: $8.04 Billion (2020)

Rob Sherman has worked at American Tower for over two decades, giving him the opportunity to build and grow the security department while strengthening both maturity and culture. He leads the team responsible for information governance, risk, and compliance, and delivers technology solutions across American Tower's global footprint.

American Tower provides the infrastructure for modern digital communications. Starting in 1995 with several thousand towers, they have grown their global portfolio to more than 200,000 communications sites. Sherman says, "In 2000, I did my job interview on a payphone. They told me - hey, we're building a data center. We think we need an email system. We've heard that you know Windows and Unix. Can you come help us out? So, I came on a six-week contract and I've stayed two decades. Today, we are a critical infrastructure provider for the major telecommunications providers on six continents, providing communications real estate, including ISO 27001 certified data center sites, worldwide."

> *"In 2000, I did my job interview on a payphone. They told me - hey, we're building a data center. We think we need an email system. We've heard that you know Windows and Unix. Can you come help us out?"*

Sherman's main responsibility is establishing security governance and overseeing how American Tower's global teams engage both in the internal organization and with their customers and vendors. He also oversees information security operations, which is different depending on the division of the company. In 2018, he worked with executive management to move the security function into the General Counsel's remit. He comments, "We wanted security to be seen as a function that, like legal, people needed to consider whenever they were making any change. We're a real estate investment trust and it made sense from a governance, risk, and compliance perspective to have the CISO function sit alongside legal."

ZERO TRUST, ISO ALIGNMENT, AND PRIVACY

Three years ago when Sherman saw some of the workforce beginning to work remotely, he began putting a larger focus on Zero Trust, which today is one of his top priorities. Not only did workforce changes impact this focus, but merger and acquisition activity became a focus for onboarding new companies quickly and securely. Sherman explains, "The next area for a lot of companies will be granular user privilege inside of Zero Trust. Once you've gotten comfortable that you're trusting the right people, the next step is figuring out how to make sure those

people can only access the very minimal set of data that they absolutely need."

Alignment to ISO 27001 is Sherman's next priority. This meets two goals, Sherman explains, "We now have customers asking us how we protect their data. Explaining to them how we've built our program in alignment with ISO 27001, along with the level of trust that comes with the certification, goes a long way towards answering that question. In addition, the Board is always interested in how we measure our cyber program. ISO 27001 controls provide an independent, third-party review which we can use to benchmark our program." He says by measuring against a framework, you are able to gauge how well your program is doing and track progress over time.

The third focus is around privacy, as countries around the world, including the United States, make traction on different laws regarding privacy. Sherman must ensure that American Tower is compliant with any new laws and they are able to respond to data requests timely and accurately. Sherman has a law degree, giving him a unique perspective and additional layer of skills and oversight to privacy regulation adherence.

OVERCOMING CHALLENGES

Luckily for Sherman and his organization, the impact of a newly remote workforce in 2020 was minimal. While many companies scrambled to set up their employees for working from home environments, Sherman and his team already had strong technologies and controls in place. He feels fortunate that this did not pose a significant challenge to his organization and security program.

However, staffing to build a top functioning team can be a challenge given the current job market conditions in this area, more so, Sherman says, than even one to two years ago. He comments, "We've leveraged good consultants to fill any gaps that arise, and that's fine, and works well to solve a point problem, but over the long term, the internal knowledge, or the relationships that an employee can build makes a real difference to the organization."

Another challenge is leading the team through constant change. Sherman says, "Identifying what the priorities are and making sure that you're picking the right ones is an ongoing exercise. Especially with the rapid evolution of threats, something that may be low priority today might become really important tomorrow. We rely on our strategy to form the foundation of our program, and we have a robust planning process, but included in that is a recognition that the nature of what we do in security requires the team to be ready for the unexpected, and that includes plans changing."

COMMUNICATING THROUGH STORIES

To communicate effectively during Board and committee

"Identifying what the priorities are and making sure that you're picking the right ones is an ongoing exercise. Especially with the rapid evolution of threats, something that may be low priority today might become really important tomorrow."

meetings, Sherman focuses on telling a story. He says, "I've approached each presentation as a story. I try to stay away from technical jargon and lots of words on slides. The Board wants to understand how you've identified risk, how you're managing risk, what they should be looking at over the next year, and how we measure ourselves. You need to be ready with the technical details if you are asked. But from what I have sensed, it seems doubtful that a Board member is especially eager for a CISO to do a deep-dive presentation on the latest data coming out of the SOC."

As a leader, Sherman says the only way cyber may become truly embedded in the culture is if everyone feels they have some level of ownership. He says, "People need to understand why the rules exist and feel like they own compliance. It's the way I've embedded it in my team. It's the way we've embedded it collectively across the company. Everyone owns a piece of company security."

IDENTITY

While internal identity presents one set of challenges, Sherman believes these are relatively manageable by ensuring the right people are on-boarded and they have access to what they need, and when they leave, that access is revoked. Since workflows similar to this have been implemented in organizations for some time, they are somewhat repeatable, requiring just minimal adjustments over time.

The new challenge for Sherman is external identities, specifically third-parties as digital transformation expands. He explains, "You have to consider suppliers, consultants, contractors, all these people accessing different pieces of your environment. And you need to build a robust platform to manage that and then maintain it. There's no one size that fits all. When building a program, we had to understand the unique needs of our different business and IT groups around the world. What we found were very use case driven, which makes it a challenge when you're building a strategy, because everyone wants to solve the use case and not focus on the strategy. We've been driving everyone to look at the digital transformation strategy and embed "Identity" in that strategy. Once we do that, implementing solutions for the use cases becomes much easier."